

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277
	)	

---

**JOINT COMMENTS OF ESCHELON TELECOM, INC., SNIP LINK INC., AND  
XO COMMUNICATIONS, INC.**

John J. Heitmann  
Jennifer M. Kashatus  
Kelley Drye & Warren LLP  
1200 19<sup>th</sup> Street, NW  
Suite 500  
Washington, D.C. 20036  
(202) 955-9600 (telephone)  
(202) 955-9792 (facsimile)

April 28, 2006

## TABLE OF CONTENTS

	Page
I. THE PROBLEM OF UNAUTHORIZED ACCESS TO DATA LIES WITH DATA BROKERS NOT TELECOMMUNICATIONS CARRIERS OR THEIR INDEPENDENT CONTRACTORS OR JOINT VENTURE PARTNERS.....	2
II. EPIC’S PROPOSALS ARE COSTLY AND BURDENSOME AND DO NOT ADDRESS THE UNDERLYING PROBLEM .....	4
A. Consumer-Set Passwords.....	5
B. Audit Trails .....	7
C. Encryption.....	8
D. Limiting Data Retention .....	8
E. Notice Requirements.....	9
III. THE FCC SHOULD NOT MODIFY ITS EXISTING OPT-OUT REGIME WITH REGARD TO JOINT VENTURE PARTNERS AND INDEPENDENT CONTRACTORS .....	11
A. There Is No Basis to Modify the Rules Pertaining to Joint Venture Partners and Independent Contractors .....	12
B. Modifying the Commission’s Rules Pertaining to Independent Contractors and Joint Venture Partners Would Have an Adverse Effect on Carriers.....	13
C. Modifying the CPNI Rules Would Violate the First Amendment of the U.S. Constitution.....	14
IV. CONCLUSION.....	16

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996	)	
	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277
	)	
	)	

---

**JOINT COMMENTS OF ESCHELON TELECOM, INC., SNIP LINK INC., AND  
XO COMMUNICATIONS, INC.**

Eschelon Telecom, Inc., SNiP LiNK Inc., and XO Communications, Inc.

(collectively, the "Joint Commenters"), through their counsel in response to the Federal Communications Commission's Notice of Proposed Rulemaking,<sup>1</sup> respectfully submit their comments in the above-captioned proceeding. The Joint Commenters have a strong incentive to protect customer proprietary network information ("CPNI"), and each has adopted stringent safeguards to protect unauthorized use of, access to, or disclosure of CPNI. To their knowledge, the Joint Commenters have not experienced security breaches through pretexting, hacking, or any other means. As such, the Commission's rules, if properly implemented, are sufficient *as they currently exist* to safeguard CPNI.

---

<sup>1</sup> See *Implementation of the Telecommunications Act of 1996*, CC Docket No. 96-115; *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*; *Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, RM-11277, Notice of Proposed Rulemaking, FCC 06-10 (rel. Feb. 14, 2006).

The Commission should not modify its CPNI rules to require carriers to comply with additional safeguards to protect the security of CPNI. In particular, the Commission should not adopt any of EPIC's proposals, each of which would be extremely onerous, particularly for competitive carriers. The Commission also must not modify its current opt-out regime with regard to joint venture partners and independent contractors, because doing so would profoundly and detrimentally impact the manner in which carriers conduct their businesses, for example, by shutting down independent sales channels thus requiring carriers to hire full-time employees to perform functions that had been performed by their independent contractors.

As demonstrated in EPIC's petition, the problem lies with unscrupulous data brokers, not telecommunications carriers. Accordingly, the Commission should enforce its existing rules and work with the Federal Trade Commission ("FTC") and other state and federal government agencies to take enforcement action against the offending parties.

**I. THE PROBLEM OF UNAUTHORIZED ACCESS TO DATA LIES WITH DATA BROKERS NOT TELECOMMUNICATIONS CARRIERS OR THEIR INDEPENDENT CONTRACTORS OR JOINT VENTURE PARTNERS**

Based on EPIC's Petition and the comments in the record, it appears that the problem that the Commission has identified—the proliferation of phone records for sale—lies almost exclusively with unscrupulous data brokers who will use any means to obtain the information that they seek. Record evidence demonstrates that data brokers have targeted certain larger carriers and contact those carriers several times a day in the guise of being a customer or a representative of the company in order to obtain CPNI.<sup>2</sup> Comments in this proceeding demonstrate that protecting the privacy of personal information is paramount to carriers, and

---

<sup>2</sup> See, e.g., EPIC Petition at 6-7; Verizon Wireless at 4 (stating that several times a day callers purport to be customers or employees to obtain information about various customer accounts).

these carriers have employed various measures to protect such information. Yet, despite the various security measures that carriers have employed, data brokers still are able to obtain information.

To the best of their knowledge, however, none of the Joint Commenters has been the victim of a security breach that has compromised CPNI. Specifically, these carriers have not discovered any internal security breaches, such as unauthorized disclosure of CPNI to third parties. The Joint Commenters also have not received any complaints from customers alleging that customer data has been misused. Nor do these carriers have reason to believe that they have been victims of pretexting, hacking, or other unlawful means of access to their CPNI. Furthermore, neither Eschelon nor XO has any reason to believe that the independent contractors and joint venture partners that they use for marketing their services either have violated their obligation to protect CPNI or have been the victim of a security breach that compromised CPNI.<sup>3</sup> The Joint Commenters have a strong incentive to safeguard their customers' CPNI, and they have implemented effective security measures to prevent the unauthorized use of, access to, and disclosure of CPNI. In response to the Commission's request,<sup>4</sup> the Joint Commenters will highlight herein certain types of protections that they have implemented to safeguard CPNI.<sup>5</sup>

Each of the Joint Commenters has implemented measures specifically designed to prevent pretexting. For example, if a customer contacts SNiP LiNK to request information about its account, then SNiP LiNK requires the customer to disclose certain identifying information beyond customer name and telephone number. In most instances, the caller would be required to

---

<sup>3</sup> SNiP LiNK does not use independent contractors or joint venture partners to market its services.

<sup>4</sup> *NPRM* ¶¶ 11, 13.

<sup>5</sup> Publicly detailing a carrier's security protection would enable a security breach and would compromise existing privacy policies.

have an actual invoice in front of him to be able to answer the identifying questions that SNiP LiNK will ask. If the caller is unable to answer the questions, then SNiP LiNK will not release any information to the caller. As an additional protection, if the customer requests a copy of an invoice, then SNiP LiNK only will send the bill via U.S. Postal Service to the contact person and billing address identified on the account.

In addition, each of the Joint Commenters has implemented, or is in the process of implementing, mandatory document destruction procedures. Under these procedures, the carriers routinely destroy information once it is no longer necessary under applicable federal and state law.

## **II. EPIC'S PROPOSALS ARE COSTLY AND BURDENSOME AND DO NOT ADDRESS THE UNDERLYING PROBLEM**

If properly implemented, the Commission's existing regulatory safeguards are adequate to protect the privacy of CPNI. As EPIC already has acknowledged, and the comments in response to EPIC's petition demonstrate, telecommunications carriers are not responsible for the current events that gave rise to EPIC's petition.<sup>6</sup> Instead, according to EPIC and the commenters, the problem lies with unscrupulous data brokers who will use any means necessary to obtain the desired information.<sup>7</sup> Accordingly, the Commission should not focus its efforts on mandating that carriers implement additional protections to safeguard CPNI, such as EPIC's proposals, but instead should enforce its existing CPNI regulations and work with the FTC and other federal and state government authorities to prevent the unauthorized access to CPNI and to

---

<sup>6</sup> See EPIC Petition at 5-6; *see also* Verizon Wireless Comments at 3.

<sup>7</sup> See EPIC Petition at 5-6; *see also* Verizon Wireless Comments at 3 (stating that it has experienced data breaches due to the practice of pretexting, whereby persons call Verizon Wireless purporting to be employees to obtain customer information).

punish the entities violating the law. The Commission also should actively enforce security breaches instead of requiring carriers to implement additional protections that are unnecessary and unworkable. The FTC already has the jurisdiction that it needs to prosecute persons who unlawfully obtain CPNI and then sell that information for profit.<sup>8</sup> By tracking down violators and enforcing penalties, the Commission should be able to curtail unlawful access to and disclosure of CPNI.

In particular, the Commission should not adopt any of the security measures that EPIC has proposed, including consumer-set passwords, audit trails, encryption, limiting data retention, and notifying consumers of security breaches. As discussed below, it would be extremely burdensome and costly for the Joint Commenters to implement any of EPIC's proposals, and implementing the proposals would not curtail the underlying problem, which is the ability of data brokers to unlawfully obtain information. If data brokers are able to obtain information with the security systems that carriers already have in place, then it is likely that they also will be able to bypass the new security measures that would be implemented in response to EPIC's petition. Furthermore, as stated above, each of the Joint Commenters already has security measures in place, which are specifically tailored to that company's use of CPNI. The Commission should not mandate a particular set of procedures for all companies. Each of EPIC's proposals is discussed below.

#### **A. Consumer-Set Passwords**

The Joint Commenters oppose the implementation of a consumer-set password protection system.<sup>9</sup> It would be extremely burdensome and costly for each of the Joint

---

<sup>8</sup> See 15 U.S.C. § 45(a) (Section 5(a) of the FTC Act authorizes the FTC to police unfair or deceptive practices).

<sup>9</sup> See *NPRM* ¶¶ 15-16.

Commenters to implement a consumer-set password protection system, and such a system would not necessarily prevent the unauthorized access to CPNI through pretexting or hacking. To properly implement a consumer-set password system, each of the Joint Commenters would need to build a database to create, house, and manage the passwords. These carriers then would need to hire full-time personnel to maintain the database, which would include collecting, and at a minimum, verifying customer passwords from every authorized user of each account, responding to customer inquiries for lost or forgotten passwords, and resetting the lost or forgotten passwords. A consumer-set password system would be particularly difficult to implement for business customers, which frequently have more than one authorized contact representative.<sup>10</sup> Depending upon the type of database implemented and the number of persons necessary to run the database, implementing and maintaining a database devoted to consumer-set passwords could impose a substantial burden on carriers, costing several hundreds of thousands of dollars per carrier.

Furthermore, consumer-set passwords are unnecessary and would not prevent unauthorized access to CPNI through pretexting or hacking. There is sufficient information in the customer account (*e.g.*, name, address, account number, telephone number, and call records) for a carrier to be able to verify a caller's identity. Moreover, this same type of customer account information would be used to legitimately reset passwords as required on an ongoing basis such that having a password will not be useful. If a caller is able to bypass the security protections that carriers already have in place, then it is likely that the caller likely would be able to bypass a password protection system. Indeed, carriers that have experienced security breaches through

---

<sup>10</sup> Moreover, customers routinely forget their passwords, and consumers that are denied legitimate access to their accounts solely will blame the carrier.



pretexting acknowledge that “[n]o combination of identifiers is safe against pretexting.”<sup>11</sup> In the end, implementing a password protected system will cost carriers millions of dollars in the aggregate, without having any beneficial effect on safeguarding information. Carriers should not be required to implement consumer-set password protections when they already have effectively less onerous security measures that are less onerous and specifically designed for their particular company.

## **B. Audit Trails**

The Joint Commenters submit that audit trails are unnecessary.<sup>12</sup> Each of the Joint Commenters already use systems that document when a customer service representative interacts with the customer account record, including situations when the customer contacts the carrier directly to request information about his or her account. Therefore, carriers already are likely to maintain records of access to customer records in one form or another. Carriers would need to spend significant resources—both time and money—to change or modify their databases so as to be able to create an audit trail. It would be extremely costly and burdensome for the Joint Commenters to change or modify their databases to develop the specific type of prescribed audit trail that the Commission proposes in the *NPRM*, and doing so would be unnecessary.<sup>13</sup> There would not be any appreciable benefits to the public by making these modifications as carriers already track this information in one manner or another.

---

<sup>11</sup> *CTIA Ex Parte* at 3 (Feb. 2, 2006) (attaching testimony by Steve Largent, President and Chief Executive Officer of CTIA, which states that CTIA is aware of cases where data brokers possessed the consumer password. For example, data brokers will scour the internet to find birth dates and social security numbers, which frequently are used as consumer passwords.).

<sup>12</sup> *See NPRM* ¶ 17.

<sup>13</sup> In some situations, carriers would not be able to modify their databases, but would be required to change their database. There would be a significant capital expense involved with changing the database. Furthermore, changing a database would take a substantial amount of time—approximately five years.

### **C. Encryption**

The Joint Commenters adamantly oppose the implementation of an encryption requirement.<sup>14</sup> Encryption is unnecessary if a carrier maintains a properly secured network. Encryption is not a workable option, because there are many instances when a carrier must unencrypt data. The carrier would need to unencrypt the data, for example, each time the customer contacts the carrier about his or her account and each time the carrier needs to service the account. Additionally, once the carrier generates data for billing purposes and issues an invoice to the customer, the encrypted data is now available in a written format outside of the carrier's system, such that there is no basis to maintain that same data in an encrypted format within the carrier's system. Furthermore, it would be extremely costly for carriers to develop a system to encrypt the data. A system capable of encrypting and decrypting data would require additional processing power and data storage space, for example, all of which translate into a substantial capital expense for the carrier to modify or change the system.

Moreover, encryption would not respond to the security concerns at the core of the Commission's *NPRM*. Based on the comments submitted in response to EPIC's petition, it appears that the data brokers predominantly access data through pretexting.<sup>15</sup> Encrypting data would not respond to this particular security concern. Accordingly, the costs of encrypting data would substantially outweigh any benefits derived from the encryption.

### **D. Limiting Data Retention**

The Commission should not implement additional data retention/data destruction regulations.<sup>16</sup> Both federal and state law (including Commission requirements) already mandate

---

<sup>14</sup> See *NPRM* ¶ 19.

<sup>15</sup> See, e.g., Verizon Comments at 2-3.

<sup>16</sup> See *NPRM* ¶ 20.

data retention for certain categories of records,<sup>17</sup> and implementing record-destruction requirements arguably could conflict with those regulations. Additionally, de-identifying records—that is, removing personally identifiable information from records—is not a realistic option, because when the carrier no longer is required to maintain the records under federal and state data retention requirements, then the carrier may prefer to destroy the records in lieu of removing certain data from the records. Furthermore, modifying carriers’ data retention policies would be extremely burdensome and potentially costly. With EPIC’s “deidentification” proposal, carriers would need to hire personnel solely devoted to scouring records to determine what information would stay in the database and what information would be deleted, thus creating an extremely time-consuming and labor intensive process. Yet, making these changes would not lead to any appreciable benefits, because there is no evidence that data brokers target older phone records, which would be the only records subject to a deidentification policy or a document destruction policy.

#### **E. Notice Requirements**

The Commission should not adopt the proposed notice requirements.<sup>18</sup> Specifically, the Commission should not require a carrier to notify consumers each time a security breach has occurred. The Commission also should not require carriers to notify customers each time that the carrier has released that customer’s CPNI. Each of these requirements is unnecessarily burdensome without a corresponding benefit.

First, the Commission should not require carriers to notify customers of each and every security breach of CPNI. Not all breaches of CPNI will result in the misuse of that information. If a CPNI security breach occurs without exposing personal or credit information,

---

<sup>17</sup> See, e.g., 47 C.F.R. §§ 42.01-.11

<sup>18</sup> See *NPRM* ¶¶ 20, 21.

then there is no risk to the customer.<sup>19</sup> Notifying the customer in this situation simply would cause the customer unnecessary alarm.

If a security breach has resulted in the breach of personally identifiable information, then the carriers already are required to notify customers under myriad federal and state rules. The Commission should not add CPNI to those disclosure requirements, as doing so would water down those requirements. Even if a security breach of CPNI has accompanied unauthorized access of personal and credit information (disclosure of which is covered by other laws), it is not necessary for the Commission to adopt rules requiring carriers to notify customers that a security breach has occurred. At least twenty-three states already have adopted customer breach notification requirements, which specify when a company must notify customers of a security breach.<sup>20</sup> More than twenty of the remaining states have pending legislation addressing this same issue, thus negating the need for the Commission to a different breach notification rule.<sup>21</sup> Furthermore, there are several pending breach notification bills in Congress.<sup>22</sup>

If, however, the Commission adopts a breach notification rule, then the Commission must limit a carrier's breach notification duties to particular circumstances. Specifically, carriers only should be required to notify customers if the particular customer's own

---

<sup>19</sup> Generally, personally identifiable information (including, for example, a social security number) is handled differently from CPNI such that a disclosure of CPNI will not necessarily result in the disclosure of personally identifiable information. Nothing in the definition of CPNI per se includes CPNI.

<sup>20</sup> For example, California's data breach notification law—the first in the country of its kind—went into effect in July 2003. Since that time, more than twenty states have adopted data breach notification laws, many of which are based on California's law.

<sup>21</sup> *See, e.g.*, Alabama, Alaska, Arizona, Iowa, Kentucky, and Virginia, among others, have pending legislation.

<sup>22</sup> *See, e.g.*, H.R. 3140, Consumer Data Security and Notification Act; S.1789, Personal Data Privacy and Security Act of 2005.

personal and credit information has been compromised; carriers should not be required to inform customers of all security breaches.

Second, carriers should not be required to notify customers routinely after every release of CPNI as the Commission proposes, whether by phone, mail (billing insert or otherwise), or electronic mail.<sup>23</sup> To provide service to their customers and to properly bill for the services that they provide, carriers routinely access customer accounts, which by their nature are composed of CPNI. Under the Commission's proposal, the carrier would be required to notify customers of each and every one of these instances, even though the carrier simply was accessing CPNI for the purpose of providing the service. Providing notification to those instances where the carrier disclosed CPNI to the purported customer also is unnecessary. It would be extremely burdensome and costly for carriers to modify their billing systems to insert a tracking component that, for example, could automatically generate a notification to include in each customer's invoice of each instance when the carrier released CPNI to the purported customer. The costs and burdens associated with notifying customers of CPNI access or disclosure, most of which would be benign, do not outweigh the substantial costs of implementing such a notification system.

### **III. THE FCC SHOULD NOT MODIFY ITS EXISTING OPT-OUT REGIME WITH REGARD TO JOINT VENTURE PARTNERS AND INDEPENDENT CONTRACTORS**

There is no rational basis for the Commission to modify its existing opt-out regime with regard to CPNI shared with telecommunications carriers' joint venture partners and independent contractors. The Joint Commenters do not have any reason to believe that either

---

<sup>23</sup> *NPRM* ¶ 23.

their joint venture partners or independent contractors are misusing, disclosing, or sharing access to CPNI outside of the scope of the arrangement with the carrier. Nor has EPIC presented any evidence that either joint venture partners or independent contractors are responsible for unauthorized use of, access to, or disclosure of CPNI. Carriers have developed their operations in reliance on existing Commission CPNI rules, and modifying the current opt-out regime would substantially impact carrier operations without the Commission or the public realizing any benefit from the modification. Furthermore, modifying the existing opt-out regime as proposed is in violation of the First Amendment of the U.S. Constitution. The Commission's existing rules are sufficient to protect the sharing of information with joint venture partners and independent contractors.<sup>24</sup>

**A. There Is No Basis to Modify the Rules Pertaining to Joint Venture Partners and Independent Contractors**

There is no evidence that either joint venture partners or independent contractors are responsible for misuse of CPNI or for unauthorized access to CPNI. Both Eschelon and XO use joint venture partners and independent contractors in their operations, including, for example, for marketing purposes. Neither company is aware of any breaches of CPNI due to the use of their joint venture partners and independent contractors. In its Petition, EPIC also did not produce any evidence demonstrating that joint venture partners or independent contractors are responsible for the unauthorized disclosure to CPNI. Based on the information set forth in EPIC's petition and in the comments submitted in response thereto, it appears that the primary misuse of CPNI can be attributed to the unauthorized access to CPNI through pretexting or

---

<sup>24</sup> The Commission's rules already require carriers and the independent contractors and joint venture partners that they hire to use specific safeguards, including, among other things, requiring the independent contractors and joint venture partners to have appropriate protections in place to safeguard confidentiality. *See* 47 C.F.R. § 64.2007(b)(ii).

hacking, and that the misuse of CPNI is not attributable to the misuse of information by joint venture partners or independent contractors.

**B. Modifying the Commission's Rules Pertaining to Independent Contractors and Joint Venture Partners Would Have an Adverse Effect on Carriers**

Modifying the current rules regarding the use of joint venture partners and independent contractors would have an adverse impact on both XO and Eschelon as well as numerous other carriers that currently use independent contractors and joint venture partners. In crafting their business models, carriers relied on the Commission's rulings made in the *CPNI Third Report and Order*,<sup>25</sup> which the Commission issued in response to the Tenth Circuit's decision in *U S West v. FCC*<sup>26</sup> vacating and remanding certain CPNI rules. Indeed, the Commission already is well aware of the detrimental impact that an opt-in scenario would have on carrier operations. In adopting joint venture and independent contractor safeguards in the *CPNI Third Report and Order*, the Commission explicitly acknowledged that "carrier burdens could be significant for these types of uses under an opt-in scenario because opt-in could immediately impact the way carriers conduct business."<sup>27</sup>

In the present case, modifying the existing opt-out regime essentially would shut down all independent sales channels. Both XO and Eschelon, as well as numerous other carriers, use joint venture partners and/or independent contractors for a variety of functions, including, sales and marketing. This practice is consistent with the Commission's previous finding that "[m]any carriers employ independent contractors such as telemarketers rather than their own

---

<sup>25</sup> *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Third Report and Order and Third Further Notice of Proposed Rulemaking, FCC 02-214 (rel. July 25, 2002) ("*CPNI Third Report and Order*").

<sup>26</sup> *U S West v. Federal Communications Commission*, 182 F.3d 1224 (10<sup>th</sup> Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000).

<sup>27</sup> *CPNI Third Report and Order* ¶ 45.

employees.”<sup>28</sup> As a practical matter, based on the Joint Commenters’ experience, if provided with an opt-in notice, customers will not exercise their right to opt-in such that the carrier may use the customer’s CPNI for marketing purposes. Therefore, carriers would be forced to hire full-time employees to perform functions that they currently outsource. In addition, companies routinely use independent contractors for certain functions related to provisioning the requested services, such as billing and collections support. The Commission should take no action that would hinder the companies from continuing to do so.

**C. Modifying the CPNI Rules Would Violate the First Amendment of the U.S. Constitution**

Requiring carriers to obtain opt-in consent prior to sharing CPNI with independent contractors and joint venture partners would violate the First Amendment of the U.S. Constitution. In adopting the current opt-in and opt-out CPNI rules, the Commission applied a First Amendment analysis as a result of the Tenth Circuit’s decision in *U S West v. FCC*.<sup>29</sup> Specifically, the Commission concluded that applying an opt-out regime for joint venture and agency use was narrowly tailored to the government’s interest in protecting consumers’ privacy.<sup>30</sup> The Commission similarly must conduct the same First Amendment analysis if it seeks to modify the opt-out rules pertaining to joint venture partners and independent contractors. As demonstrated herein, however, applying an opt-in regime to a carrier’s ability to share CPNI with its independent contractors and joint venture partners would violate the First Amendment, because it is not narrowly tailored to the Commission’s objective of protecting consumer privacy.

---

<sup>28</sup> *Id.* at note 121.

<sup>29</sup> *CPNI Third Report and Order* ¶¶ 26-30; 39-44 (citing and applying the court’s decision in *U S West v. FCC*, 182 F.3d 1224 (10<sup>th</sup> Cir. 1999)).

<sup>30</sup> *Id.* ¶ 30.



The Tenth Circuit previously has vacated the Commission's rules pertaining to CPNI and set forth the applicable framework upon which the Commission should evaluate subsequent CPNI rules. In *U S West v. FCC*, the Tenth Circuit vacated the Commission's prior attempt to mandate an opt-in regime,<sup>31</sup> holding that the Commission's CPNI rules violated the First Amendment by impermissibly regulating protected commercial speech. In deciding *U S West v. FCC*, the court applied the four part constitutional standard articulated in *Central Hudson Gas & Elec. Corp. v. Public Service Commission*:<sup>32</sup> (1) whether the speech in question concerns illegal activity or is misleading, in which case the government may freely regulate the speech; if the speech is not illegal or misleading, then the court applies the rest of the test to the FCC's regulations; (2) whether the government has a substantial interest in regulating the speech; (3) whether the government can demonstrate that the restriction on commercial speech directly and materially advances that interest; and (4) whether the regulation is narrowly drawn. The court held that although the Commission had demonstrated a privacy interest, the Commission failed to satisfy the third and fourth prongs of *Central Hudson*. Specifically, the court found that the Commission had not presented any "[empirical] evidence showing the harm to either privacy or competition is real."<sup>33</sup> The court also found that the Commission's opt-in regime was not narrowly tailored to achieving the Commission's objective.<sup>34</sup>

In the present case, applying an opt-in regime for independent contractors and joint venture partners also would violate the First Amendment. The Commission cannot satisfy the four-part test set forth in *Central Hudson*, which is equally applicable in this context. There

---

<sup>31</sup> *U S West v. FCC*, 182 F.3d at 1224.

<sup>32</sup> *Central Hudson Gas & Elec. v. Public Service Commission*, 447 U.S. 557 (1980).

<sup>33</sup> *Id.* at 1237.

<sup>34</sup> *Id.* at 1238-39 (noting that it was "difficult, if not impossible" for the court "to conduct a full and proper analysis given the deficiencies that [the court] already [has] encountered with respect to the previous portions of the *Central Hudson* test.").

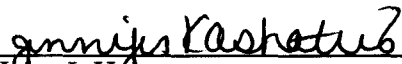
is no question that the speech in question is neither illegal nor misleading such that the Commission has a free reign on regulating the speech; therefore, the remaining components of *Central Hudson* are applicable. The Joint Commenters also do not dispute that the Commission has a substantial interest in protecting privacy.

The Commission's proposed opt-in regime, however, fails the third and fourth prongs of the test as it did in *US West v. FCC*: the Commission cannot demonstrate that the restriction on commercial speech directly and materially advances its interest. As discussed above, there is no evidence demonstrating that joint venture partners or independent contractors are responsible for the abusive CPNI practices that are of concern to the Commission. A court would be compelled to make the same finding in this case as the Tenth Circuit reached in *US West v. FCC*; that is, there is no evidence showing that the harm to privacy and competition is real absent an opt-in regime applicable to joint venture partners and independent contractors. Furthermore, subjecting a carrier to an opt-in regime in its dealings with independent contractors and joint venture partners is not narrowly tailored with the objective to protect consumer privacy. Accordingly, any regulation mandating an opt-in regime with regard to joint venture partners and independent contractors would be in violation of the First Amendment.

#### IV. CONCLUSION

For the foregoing reasons, the Commission should not modify its existing CPNI rules, but instead should enforce its existing rules and work with the FTC and other state and federal regulatory agencies to curtail unlawful access to and disclosure of CPNI.

Respectfully submitted,

  
\_\_\_\_\_  
John J. Hejtmann  
Jennifer M. Kashatus  
Kelley Drye & Warren LLP  
1200 19<sup>th</sup> Street, NW  
Suite 500  
Washington, D.C. 20036  
(202) 955-9600 (telephone)  
(202) 955-9792 (facsimile)

April 28, 2006

**CERTIFICATE OF SERVICE**

I, Tara Keilberg, hereby certify that on this 28<sup>th</sup> day of April, 2006, I served a true and correct copy of Joint Comments of Eschelon Telecom, Inc., SNiP LiNK Inc., and XO Communications, Inc. via the Commission's electronic filing system, unless otherwise noted.

Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D.C. 20554  
(Public version only)

Janice Myles^  
Competition Policy Division  
Wireline Competition Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Room 5-C140  
Washington, D.C. 20554

Best Copy and Printing, Inc. (BCPI)^  
Portals II  
445 12<sup>th</sup> Street, SW  
Room CY-B402  
Washington, D.C. 20554

Chris Jay Hoofnagle\*  
Electronic Privacy Information Center  
West Coast Office  
944 Market Street, #709  
San Francisco, CA 94102

  
Tara Keilberg

\* Via Overnight Mail

^ Via email